

Banco de Dados Segurança



Professor: Carlos Alberto
Email: carloswgama@gmail.com

Preparando Ambiente

- Use o mesmo schema da aula passada **aula_seguranca**.

- Caso não tenha criado, crie com os comandos abaixo:

```
CREATE DATABASE  
aula_seguranca;
```

- Após criado, execute os comandos do script da aula ou do link abaixo:

[https://pastebin.com/raw/
jtjq8rtu](https://pastebin.com/raw/jtjq8rtu)

Segurança

Segurança em um Banco de Dados

- Os Bancos de Dados costumam guarda informações muito importantes de usuários como senhas, endereço, telefones, contas bancárias e número de cartões, por isso é sempre importante realizar uma boa configuração de segurança ao acesso ao banco visando.
- Para isso podemos criar:
 - Usuários – Usuários que tem certos privilégios a uma banco ou tabela;
 - Grupos – Grupo de usuários que podem ter mesmos privilégios para interagir com tabela;

Criando usuário

- Para se criar um usuário, pode-se usar o comando `CREATE USER`.
- Porém tudo dentro do PostgreSQL também é considerado um Role (Papel). Por também podemos usar o comando `CREATE ROLE`.
- Nas ultimas versões o comando `CREATE USER` virou um simples alias de compatibilidade para o `CREATE ROLE`.

Criando Usuário

- Para criar um novo usuário, basta usar o comando:

```
CREATE ROLE nome_do_papel [WITH  
opções]
```

```
CREATE USER nome_do_papel [WITH  
opções]
```

O comando `WITH` é opcional para separar as opções do login do usuário

```
CREATE ROLE admin WITH LOGIN SUPERUSER PASSWORD  
'12345';
```

```
CREATE USER usuario WITH PASSWORD  
'xxxxxxx';
```

Opções do Usuário

Comando	Descrição	Padrão
SUPERUSER ou NOSUPERUSER	Dar ou não o direito de super-usuário ao papel. Um Super-usuário pode fazer qualquer coisa no sistema.	NOSUPERUSER
CREATEDB ou NOCREATEDB	Dar ou não permissão de criar bancos	NOCREATEDB
CREATEROLE ou NOCREATEROLE	Dar ou não a permissão de criar novos papeis	NOCREATEROLE
LOGIN ou NOLOGIN	Permite ou não o papel realizar um login. Caso dê a permissão de LOGIN, a role é considerada um usuário	NOLOGIN (No ROLE) LOGIN (No USER)
PASSWORD 'senha'	Informa senha do usuário	
CONNECTION LIMIT valor	Quantas conexões simultâneas o papel pode ter, caso deseje não por limites, usar -1 no valor	-1
VALID UNTIL 'ANO-MÊS-DIA HORAS:MINUTOS:SEGUNDOS'	Define um período que a role irá expirar e não poderá mais ser usada. Caso não queira uma data de expiração usar 'infinity'	Infinity

Alterando Usuário

- Para alterar um usuário existente usar:

```
ALTER ROLE nome_do_papel [ WITH opções que deseja  
mudar]
```

```
ALTER USER nome_do_papel [ WITH opções que deseja  
mudar]
```

```
ALTER ROLE admin WITH PASSWORD  
'123456';
```

```
ALTER ROLE usuario WITH VALID UNTIL '2017-12-  
30';
```

Excluir Usuário

- Para apagar um usuário existente, use:

```
DROP ROLE
```

```
nome_do_papel
```

```
DROP USER
```

```
nome_do_papel
```

Exemplo:

```
DROP ROLE admin
```

```
DROP USER
```

```
usuario
```

Exercício

- Crie os 3 usuários a seguir:

Nome	Senha	Adicionar opção
coordenador1	123456	Login e Permitir criar usuário
professor1	123456	Login
aplicativo_mobile	123456	Login e válido até '2020-12-31'

```
CREATE USER coordenador1 PASSWORD '123456' CREATEROLE;  
CREATE USER professor1 PASSWORD '123456';  
CREATE USER aplicativo_mobile PASSWORD '123456' VALID UNTIL '2020-12-31';
```

Criando um grupo

- Para criar um novo grupo, basta fazer:

```
CREATE GROUP nome_do_grupo;
```

```
CREATE ROLE nome_do_grupo;
```

Exemplo:

```
CREATE GROUP  
testadores;
```

```
CREATE ROLE  
desenvolvedores;
```

Também é possível usar o CREATE USER para criar grupos (Usando a opção NOLOGIN) assim como o CREATE GROUP para criar usuários (Usando a opção LOGIN) embora não seja uma boa prática.

Também não é uma boa prática criar grupos para super-usuários ou as demais opções de usuário. Usaremos group apenas para definir permissões sem tabela

Alterando membros do grupo

- Para adicionar um membro do grupo, obrigatoriamente temos que usar o ALTER GROUP:

```
ALTER GROUP nome_do_grupo ADD USER nome_da_role;
```

Exemplos:

```
ALTER GROUP testadores ADD USER  
usuario1;
```

```
ALTER GROUP testadores ADD USER usuario2,  
grupo2;
```

- Para remover usuários/grupos usar o comando:

```
ALTER GROUP nome_do_grupo DROP USER  
nome_da_role;
```

```
ALTER GROUP testadores DROP USER  
usuario1;
```

Excluindo um grupo

- Para excluir um grupo usar:

```
DROP GROUP nome_do_grupo
```

```
DROP ROLE nome_do_grupo
```

Exemplo:

```
DROP GROUP  
testadores;
```

Exercício

- Crie um grupo “professores” e adicione o professor1 ao grupo professores:

```
CREATE GROUP professores;  
ALTER GROUP professores ADD USER  
professor1;
```

- Crie um grupo coordenadores e adicione o coordenador1 ao grupo coordenadores

```
CREATE GROUP coordenadores;  
ALTER GROUP coordenadores ADD USER  
coordenador1;
```

Definindo privilégios em Tabelas

- Após criar os grupos e usuários desejados a utilizarem o sistema, é possível adicionar privilégios a determinado banco ou tabela.
- Os privilégios mais usados nas tabelas são:

Privilégio	Descrição
SELECT	Permite fazer buscas na tabela
INSERT	Permite inserir dados a tabela
UPDATE	Permite atualizar dados da tabela
DELETE	Permite excluir dados da tabela
REFERENCES	Permite criar chaves estrangeiras para a tabela
TRUNCATE	Permite zerar os dados da tabela
ALL PRIVILEGES	Permite fazer qualquer coisa na tabela. O nome PRIVILEGES é opcional

Definindo privilégios em Bancos

- Os privilégios mais usados nos bancos de dados são:

Privilégio	Descrição
TEMP ou TEMPORARY	Permite criar tabelas temporárias
CREATE	Permite criar tabelas

Apenas os donos banco ou super-usuários podem excluir tabelas

Dando privilégios na tabela

- Um privilégio pode ser dado a um grupo de usuário ou usuário através do comando:

```
GRANT privilegios_tabela ON nome_tabela TO  
nome_usuario;
```

```
GRANT privilegios_banco ON DATABASE nome_banco TO  
nome_usuario;
```

Exemplos:

```
GRANT SELECT, INSERT, UPDATE ON tabela TO  
usuario1;
```

```
GRANT ALL PRIVILEGES ON tabela TO  
grupo1;
```

```
GRANT CREATE ON DATABASE banco1 TO usuario1,  
grupo1;
```

Retirando privilégios

- Um privilégio pode ser retirado de um grupo de usuário ou usuário através do comando:

```
REVOKE privilegios_tabela ON nome_tabela FROM  
nome_usuario;
```

```
REVOKE privilegios_banco ON DATABASE nome_banco FROM  
nome_usuario;
```

Exemplos:

```
REVOKE SELECT, INSERT, UPDATE ON tabela FROM  
usuariol;
```

```
REVOKE ALL ON tabela FROM  
grupo1;
```

```
REVOKE CREATE ON DATABASE banco1 FROM usuariol,  
grupo1;
```

Exercício

- Usando o banco de dados disponibilizado no portal, adicione as seguintes permissões aos usuários ou grupos:

Usuário/Grupo	Permissões	Tabela
coordenadores	SELECT INSERT UPDATE DELETE	alunos
coordenadores	SELECT INSERT UPDATE DELETE	notas
professores	SELECT INSERT UPDATE	alunos
professores	SELECT INSERT UPDATE	notas
aplicativo_mobil e	Tudo	notas

Exercício

- Resultado:

```
GRANT SELECT, INSERT, UPDATE, DELETE ON notas TO  
coordenadores;  
GRANT SELECT, INSERT, UPDATE, DELETE ON alunos TO  
coordenadores;  
GRANT SELECT, INSERT, UPDATE ON notas TO professores;  
GRANT SELECT, INSERT, UPDATE ON alunos TO professores;  
GRANT ALL ON notas TO aplicativo_mobile;
```

- Retire a permissão dos professores de atualizar e inserir dados na tabela alunos

```
REVOKE UPDATE, INSERT ON alunos FROM  
professores;
```